Methods of information systems protection

UDC 004. 6 **doi:** https://doi.org/10.20998/2522-9052.2022.4.10

Serhii Semenov[1], Min Jian Zhang[2]

[1] Kharkiv National economic university named after S. Kuznets, Kharkiv, Ukraine
[2] Zhejiang Nova Intelligent Technology Co. Ltd, Zhejiang, China

COMPARATIVE STUDIES OF METHODS FOR IMPROVING THE CYBER SECURITY OF UNMANNED AERIAL VEHICLES WITH THE BUILT-IN ADS-B SYSTEM

Abstract. The subject of study in the article is methods for improving the cybersecurity of unmanned aerial vehicles with an integrated ADS-B system. The aim is to analyze and compare methods for improving the cybersecurity of unmanned aerial vehicles with an embedded ADS-B system. Particular scientific tasks: analysis and comparative studies of the main types of cyber threats and methods for improving the cybersecurity of unmanned aerial vehicles with an integrated ADS-B system, the development of an appropriate taxonomy, and the development of proposals for further research. The methods used in the article are the methods of system analysis. The following research results have been obtained: a classification of cyber threats to the security of unmanned aerial vehicles with an integrated ADS-B system has been developed; a taxonomy of ADS-B message modification and injection attacks has been developed; practical UAV security metrics adapted to the presented taxonomy of cyberattacks are defined and researched ; chosen most priority directions research ; - a generalized classification of cryptographic protection methods adapted to solve the problems of improving the security of UAVs with an integrated ADS-B system has been developed; the use of additional means of identification based on steganographic methods of data protection is proposed. Conclusions. An analysis and comparative studies have been carried out, and a generalized classification of methods for improving the cybersecurity of unmanned aerial vehicles with an integrated ADS-B system has been developed. Their advantages and disadvantages are revealed, which made it possible to determine the priority of further research and possible promising ways to solve the tasks.

Keywords: Unmanned aerial vehicles; security; ADS-B system; cyber-attacks; data protection.

Introduction

Recently, there has been a significant interest in software-defined radio (SDR) technology in the circles of developers of methods and means of air traffic control [1]. The idea of using the hardware functions of radio communications with the help of software tools has received practical application and recognition in matters of dynamic optimization of the used spectrum. As a result of research, in 2010 the US Federal Aviation Administration (FAA) published the Automatic Dependent Surveillance-Broadcast (ADS-B) regulations. Feature requirements. Air traffic control support" [2]. This provision prescribes the equipping of aircraft of a certain class with the ADS-B system.

The increased attention of air traffic control managers to ADS-B technology has forced manufacturers to accelerate the process of introducing related equipment. And already most aircraft manufacturers are equipping their models with the ADS-B system.

With a slight delay, but at no less pace, in recent years, the process of introducing ADS-B systems into unmanned aerial vehicles (UAV) equipment has been observed.

However , this rapid incorporation of the latest air traffic monitoring technology into aircraft equipment has simultaneously exposed issues of near-total insecurity in the data exchange process. ADS-B sends packets in the clear, which makes the system vulnerable to confidentiality, integrity, availability, and ownership attacks.

Literature analysis. The work [3] presents an analytical report that fixes the great interest of developers in the security issues of the ADS-B technology. Possible ways to improve security and ensure confidentiality using symmetric and asymmetric encryption mechanisms are indicated. However, the lack of references to real cyber-attacks and cyber incidents , as well as the uncertainty about security requirements, reduces the practical value of this material.

Article [4] presents an analysis of the security requirements for ADS-B networks. However, the materials presented in the article are adapted to the conditions for performing the flight mission of aircraft and helicopters. At the same time, the flight characteristics of UAVs have a significant difference in comparison with airplanes and helicopters. This should automatically be reflected in changes in characteristics and their safety requirements.

Article [5] presents the results of a study of the vulnerabilities of the ADS-B system. Also in this paper, a number of countermeasures aimed at reducing the risks of cyberattacks are analyzed . But, as the authors of the article themselves emphasized, the paper does not present proposals for substantiating the most priority areas for studying the safety of aircraft with the ADS-B system. In addition, all the examples considered are mostly related to controlled aircraft (airplanes and helicopters), and do not affect the problems of UAVs.

It should be noted that most of the scientific research at this stage is aimed at ensuring the confidentiality of the service data of the ADS-B system. So, for example, in [6] the algorithm of cryptographic protection of transmitted data is considered separately. At the same time, the technology of complex use of symmetric and asymmetric encryption is taken as a basis. However, the complexity of the exchange of key information, together with unsolved problems of data exchange speed and, accordingly, effective identification, allow us to con-

clude that there is a more effective solution to the UAV security problem with the ADS-B system.

In [7], the issue of identifying the ADS-B system and possible threats to this process are considered. However, the material of the article describes the issue with reference to aircraft. Features of the UAV flight mission are not considered in the work.

Thus, we can note the relevance of the problem of improving the safety of UAVs with the built-in ADS-B system. An important initial stage of research, at the same time, is the analytical study of the cyber threats of UAVs with the built-in ADS-B system, together with proposals for the most effective ways to solve the problem of improving its security .

Main part

The results of studies of most known cyber-attacks on UAVs through the built-in ADS-B system showed the possibility of classifying them into the following vulnerability sectors: ground sector; air sector [8].

The terrestrial attack sector includes: ADS-B terrestrial networks (including data links and terrestrial stations UAV control), distributed computer networks, a common ground air traffic control point.

The air attack sector includes: the onboard ADS-B system of the UAV, the air-to-ground sector, the ADS-B data transmission medium of the UAV.

Among the cyberattacks , the following can be distinguished : interception and control of signals in the ADS-B OUT of the UAV, modification of messages, forced injection of messages .

The conducted studies have shown that the interception and control of UAV ADS-B Out signals can be performed by any commercially available ADS-B receiver. At the same time, aircraft surveillance, reconnaissance and eavesdropping are performed. The target sector of this cyber-attack is the air sector (air-to-ground). Technically, the attack is performed by jamming, disrupting the transmission of the RF channel and / or GPS signals to the A / C. With a low level of complexity and relatively low cost, the impact is very serious. Especially in congested airspaces and adverse weather conditions.

Studies have shown that the integrity of the ADS-B message is also a very important security feature. Therefore, a "message modification" cyber-attack is also very commonly used by cyber attackers . When implemented, the attacker must correctly calculate the time and position for sending the message modification. At the same time, by obscuring the signal, we can interfere with the attacker, as it is easier to decode the message without errors. This property can be used when implementing UAV protection methods with the built-in ADS-B system.

Another dangerous type of cyberattack on UAVs with an embedded ADS-B system is message injection. This type of attack can take many forms: GPS/RF signal jamming, UAV spoofing , and ghost UAV.

When jamming GPS and RF signals, hackers send an unmanageable amount of messages to saturate the communication channel. This may disable one or more wireless network nodes from sending or receiving messages with sufficient power. The target of the attack is both the air segment and the air-to-ground segment. As in the first case, this type of attack at low cost can cause a large number of negative consequences in congested airspaces.

Recently, one of the most common attacks has become the UAV spoofing attack. In this type of cyberattack , a hacker eavesdrops on an RF channel in order to interpret messages and interfere with the desired message. It should be noted that the range of negative results of this cyber-attack is very wide: from the loss (theft) of UAVs to a serious increase in the workload of air traffic controllers.

One of the most dangerous cyberattacks on UAVs, in recent years, researchers consider an attack of the “Ghost UAV” type. When implementing such an intrusion , cybercriminals enter reliable data into the UAV control system so that the recipient cannot identify the "ghost" as a fake. A technique for such an attack is to insert a message containing a valid date that appears to be present in the control system of the real UAV. The severity of such an attack is caused by an increase in the load on the UAV control system or operators when trying to identify by other means a possible real flying machine. This can significantly affect the trajectory of the UAV and the performance of the flight task.

It should be noted that despite the high activity of intruders and a wide range of possible attacks, researchers offer a number of solutions that can improve the security of UAVs. However, the lack of consistency in their solution significantly reduces the effectiveness of the practical implementation of these developments.

To highlight priority areas in solving security problems, developers very often need to present a taxonomy of UAV cybersecurity threats with built-in ADS-B. The paper proposes the following taxonomy of ADS-B message modification and injection attacks .

Cyber-attacks are divided into three classes, classified depending on the complexity of implementation, the location of the radio station, and the means of the attacker . These classes are the following:

1. Medium attacks. In this type of attack, the attacker generates malicious ADS-B messages that are usually entered randomly. In this case, the attacker uses stationary equipment. An example would be an attack where a hacker sends a huge amount of ADS-B messages with a fake ID. ADS-B equipment is within reach ATC Sever .

2. Advanced attacks. In these attacks, the attacker uses sophisticated flight simulator programs along with a radio device to send a more realistic flight path that cannot be easily detected as a fake. For example , for this can use one of popular programs – Flight Gear [9]. In this case, the location of the equipment used to attack the UAV is fixed in order to block the view of the radar display and thus prevent the UAV operator from performing his duties.

3. Expert level attacks. This type of attack is similar to advanced level attacks, except for the fact that the equipment used to launch the attack is on a UAV. Such an attack is more difficult to test as it requires complex equipment and procedures.

Such a taxonomy of cyberattacks on UAVs requires the analysis and synthesis of indicators necessary to decide whether a particular cyberattack belongs to a certain class modeled in the ontology rule. Using the data of the article [10], we define three security metrics.

1. The difference is in the location of the sender. Absolute value difference between triangulated location sender in two consecutive moment time t_i and t_j . Let's assume that we have the appropriate triangulation tools needed to determine the location of the sender based on the received ADS-B message. This metric is divided into three sub- metrics , which are correspond difference between longitude, latitude and altitude.
2. Speed at time t .
3. The difference between the calculated and actual location of the UAV. The absolute value of the difference between the estimated position of the UAV and the position obtained from the ADS-B packet at time t . Assume the possibility of estimating the location of the UAV at any time. This metric is also from three submetrics corresponding to differences longitude, latitude and altitude.

Conducted studies have shown that these three parameters can be used in the analysis of cyber threats to the ADS-B system. These metrics synthesize actionable attack data and allow the security analyst to categorize cyberattacks based on patterns of anomalous behaviour.

The listed parameters are used by the Pellet platform [11] for automatic classification of the type of attack. The relationship between the three specified attack classes and security metrics can be described as follows.

Medium-level attacks can be qualified if the difference in the location of the UAV, as well as its speed, is zero. An UAV whose physical location does not change can be referred to as a ghost UAV. In addition, the difference between the calculated and real indicators of longitude, latitude and height should be different. Therefore, if the location obtained from the ADS-B packet is not fixed in the UAV coverage area, then such a packet can be considered compromised.

An advanced level attack can be qualified if the difference in the UAV's location as well as the speed is zero . But, at the same time, the difference between the calculated and real indicators of longitude, latitude and height can be within predetermined threshold values. An expert-level attack implies that the speed indicators obtained from the message are comparable to the speed of a real UAV. In addition, the difference in the difference between calculated and actual longitude, latitude and altitude may be within predetermined thresholds.

Based on the presented data, it is possible to form a classification of UAV cyber threats with an integrated ADS-B system (Table 1). This classification will allow us to choose most priority directions research.

Table 1 – **Classification of cyber threats of UAVs with an embedded ADS-B system**

Type of attack	Complexity	Effects	Assessment Metrics	Methods opposition	Priority
UAV ADS-B Out signals	Low	Introducing RF Transmission Errors and A/C GPS Interference	Sender location difference	Optimization of the architecture and structure of radio frequency channels, the use of modern error-correcting codes and noise-protected signals	Medium
Message modification	Medium	Introduction of uncertainty into information about the air situation	The difference is in the location of the sender. UAV speed.	Signal obscuration, use of cryptographic and steganographic protection tools	High
Jamming GPS/RF signals	Low	Disable one or more wireless hosts from sending or receiving messages	The difference between the calculated and actual location of the UAV.	Use of special equipment	Medium
UAV spoofing	Medium	Loss (theft) of UAVs, increase in the workload of air traffic controllers	The difference is in the location of the sender. UAV speed. The difference between the calculated and actual location of the UAV.	Use of cryptographic and steganographic security tools	High
Ghost UAV	Medium	Increased load on the UAV control system or operators when trying to identify by other means a possible real flying machine	The difference is in the location of the sender. UAV speed. The difference between the calculated and actual location of the UAV.	Use of cryptographic and steganographic security tools	High

As can be seen from Table 1, to reduce the risk of cyber attacks on UAVs, a number of cryptographic protection approaches are currently used. A generalized classification of cryptographic protection methods adapted to solve the problems of improving the security of UAVs with an integrated ADS-B system is presented in Table. 2.

It should be noted that in these analytical materials there is no information about the possibilities of steganographic methods for improving data security. How-

ever, according to the authors of the article, it is this technology that has been highly appreciated by researchers and can become a promising direction in improving the safety of UAVs. Therefore, the authors associate further research with the development and research of methods and means of steganographic data protection to improve the safety of UAVs with an integrated ADS-B system.

Table 2 – **Generalized classification of cryptographic protection methods adapted to solve the problems of improving the security of UAVs with an embedded ADS-B system**

Methods cryptographic protection	Advantages	Flaws
PKI, symmetric and asymmetric encryption methods. It used a Public Key Infrastructure (PKI) to verify all ADS-B signals from the UAV, a symmetric session key for authentication and data integrity [12].	UAV identification and ADS-B message authentication. Reducing the risk of tracking the public key by third parties. Reducing the number of digital signatures.	Requires software updates and MAC address in the package. Increased load on public key generation; poses a threat if the private key is used.
Hashing algorithms, asymmetric and symmetric encryption of ADS-B signals [13].	Increased speed through the use of fast hashing algorithms. Reducing the number of software updates	Introduction of extra bits in ADS-B messages. Difficulty in exchanging public keys between nodes, which requires knowledge of the recipient before sending the message. Security issues in key distribution. More testing under collision and simulation conditions is required.
Phased identification based on encryption [14].	Privacy Compliant	Doesn't meet authentication requirements
Three-Level Identity-Based Hierarchical Signature (HIBS) [15].	Meets authentication requirements	High requirements for equipment. Increased credential requirements.
Using HIBE with Diffie clauses Hellmanin [16].	Increases security	Low efficiency
Using the Lewko technique with anonymous identity-based encryption schemes [17].	Mitigating Attacks with Full Adaptive Identity	Increased risk of master key leakage if it is used by untrusted sources
NextGen air traffic control system [18].	Incorporate air traffic control and academia into the process	Server limitations and complexities of eventual integration between ADS-B and air traffic control system

Conclusions

Analysis of the main types of cyber-attacks on UAVs with the built-in ADS-B system was carried out. Based on the results of the analysis, a classification of relevant cyber threats has been developed .

A taxonomy of ADS-B message modification and injection attacks has been developed.

Practical UAV security metrics adapted to the presented taxonomy of cyberattacks are defined and researched.

The metrics presented synthesize practical attack data and allow the security analyst to categorize cyberattacks based on patterns of anomalous behaviour.

Presented classification cyber threats allowed to choose most priority directions research .

An analysis and comparative studies have been carried out, and a generalized classification of cryptographic protection methods adapted to solve the problems of improving the security of UAVs with an integrated ADS-B system has been developed.

The results of the analysis of cryptographic data protection methods made it possible to draw conclusions about their shortcomings in the conditions of use to improve the security of UAVs.

As one of the ways to solve these problems, it was proposed to use additional means of identification based on steganographic data protection methods.

REFERENCES

1. Krishnan, Rahul & Rajendran, Ganesh Babu & Kaviya, S. & Kumar, N. & Rahul, C. & Raman, S. (2017), "Software defined radio (SDR) foundations, technology tradeoffs: A survey", *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering* (ICPCSI), pp. 2677-2682, doi: https://doi.org/10.1109/ICPCSI.2017.8392204.
2. (2010), *14 CFR Part 91, Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service*; Final Rule. May 28, 2010, ICC.
3. Alghamdi, Fatimah, Alshhrani, Amal & Hamza, Nermin (2018), "Effective Security Techniques for Automatic Dependent Surveillance-Broadcast (ADS-B)", *International Journal of Computer Applications*, Vol. 180, pp. 23–28, doi: https://doi.org/10.5120/ijca2018916598.
4. Kacem, Thabet, Wijesekera, Duminda, Costa, Paulo & de Barros Barreto, Alexandre (2014), "Security requirements analysis of ADS-B networks", *CEUR Workshop Proceedings*, 1304, pp. 40–47, available at: https://ceur-ws.org/Vol-1304/STIDS2014_T06_KacemEtAl.pdf.
5. Manesh, Mohsen Riahi & Kaabouch, Naima (2017), "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system", *International Journal of Critical Infrastructure Protection*, 19, doi: https://doi.org/10.1016/j.ijcip.2017.10.002.

6. Strohmeier, Martin, Lenders, Vincent & Martinovic, Ivan (2013), “Security of ADS-B: State of the Art and Beyond”, *IEEE Communications Surveys & Tutorials*, 17, doi: https://doi.org/10.1109/COMST.2014.2365951.
7. Purton, Leon, Abbass, Hussein & Alam, Sameer (2010), “Identification of ADS-B System Vulnerabilities and Threats”, *ATRF 2010: 33rd Australasian Transport Research Forum*, pp. 1–16.
8. John, Perkaus (2020), *ADS-B Cyber Security alert*, available at: https://www.perkausandfarley.com/wp-content/uploads/2022/01/ADSBCyberSecurity.pdf.
9. Purvis, A., Morris, B. and McWilliam, R., (2015), “FlightGear as a Tool for Real Time Fault-injection, Detection and Selfrepair”, *Procedia CIRP*, vol. 38, pp. 283-288
10. (2013), “MITRE’s Making Security Measurable”, *MITRE’s Making Security Measurable*, available at: http://makingsecuritymeasurable.mitre.org.
11. Sirin, E., Parsia, B., Grau, B. C., Kalyanpur, A. and Katz, Y. (2007), “Pellet: A practical OWL-DL reasoner”, *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 51–53.
12. Cook, E. (2015), "ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft", *2015 IEEE 17th International Conference on High Performance Computing and Communications*, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, 2015, pp. 1256-1261, doi: https://doi.org/10.1109/HPCC-CSS-ICESS.2015.201.
13. Amin, S., Clark, T., Offutt, R. and Serenko, K. (2014), "Design of a cyber security framework for ADS-B based surveillance systems", *2014 Systems and Information Engineering Design Symposium* (SIEDS), pp. 304-309, doi: https://doi.org/10.1109/SIEDS.2014.6829910.
14. Hableel, E., Baek, J., Byon, Y. -J. and Wong, D. S.(2015), "How to protect ADS-B: Confidentiality framework for future air traffic communication", *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 155–160, doi: https://doi.org/10.1109/INFCOMW.2015.7179377.
15. Debiao, He, Kumar, Neeraj, Choo, Kim-Kwang Raymond & Wu, Wei (2016), “Efficient Hierarchical Identity-Based Signature With Batch Verification for Automatic Dependent Surveillance-Broadcast System”, *IEEE Transactions on Information Forensics and Security*, pp. 454–464, doi: https://doi.org/10.1109/TIFS.2016.2622682.
16. Anjia, Y., Xiao, T., Joonsang, B. and Duncan, S. W. (2017), “A New ADS-B Authentication Framework Based on Efficient Hierarchical Identity-Based Signature with Batch Verification”, *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165-175, March-April, doi: https://doi.org/10.1109/TSC.2015.2459709.
17. Hao, W., Zhihua, Z. and Lei, W. (2014), “Hierarchial Identity-Based Encryption Scheme from Multilinear Maps”, Tenth International Conference on Computational Intelligence and Security, Kunming, pp. 455–458.
18. Strohmeier, M., Schäfer, M., Lenders, V. and Martinovic, I. (2014), “Realities and challenges of nextgen air traffic management: the case of ADS-B”, *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111-118, May 2014, doi: https://doi.org/10.1109/MCOM.2014.6815901.

Received (Надійшла) 31.08.2022
Accepted for publication (Прийнята до друку) 23.11.2022

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Семенов Сергій Геннадійович – доктор технічних наук, професор, професор кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені С. Кузнеця, Харків, Україна;
Serhii Semenov – Doctor of Technical Sciences, Professor, Professor of Department cyber security and information technologies, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: s_semenov@ukr.net; ORCID ID: http://orcid.org/0000-0003-4472-9234.

Мін Цзянь Чжан – здобувач, Co. Ltd “Нові інтелектуальні технології Чжецзяна”, Чжецзян, Китай;
Min Jian Zhang – degree applicant, Zhejiang Nova Intelligent Technology Co. Ltd, Zhejiang, China;
e-mail: minjianzhang.s@gmail.com; ORCID ID: https://orcid.org/0000-0002-4143-1689.

Порівняльні дослідження методів підвищення кібербезпеки безпілотних апаратів з вбудованою системою ADS-B

С. Г. Семенов, Мін Цзянь Чжан

Анотація. Предметом вивчення у статті є методи підвищення кібербезпеки безпілотних літальних апаратів із вбудованою системою ADS-B. Метою є аналіз та порівняльні дослідження методів підвищення кібербезпеки безпілотних літальних апаратів із вбудованою системою ADS-B. Приватні наукові завдання: аналіз та порівняльні дослідження основних видів кіберзагроз та методів підвищення кібербезпеки безпілотних літальних апаратів із вбудованою системою ADS-B, розробка відповідної таксономії, а також розробка пропозицій подальших досліджень. Методами, що використовуються в статті, є методи системного аналізу. Отримано наступні результати досліджень: розроблено класифікацію кіберзагроз безпеки безпілотних літальних апаратів із вбудованою системою ADS-B; розроблено таксономію кібератак модифікації та примусового впровадження повідомлень ADS-B; визначено та досліджено практичні метрики безпеки БПЛА, адаптовані до представленої таксономії кібератак; обрано найбільш пріоритетні напрями дослідження; розроблено узагальнену класифікацію методів криптографічного захисту, адаптованих для вирішення завдань підвищення безпеки БПЛА з вбудованою системою ADS-B; запропоновано використання додаткових засобів ідентифікації на основі методів стеганографії захисту даних. Висновки. Проведено аналіз та порівняльні дослідження, а також розроблена узагальнена класифікація методів підвищення кібербезпеки безпілотних літальних апаратів із вбудованою системою ADS-B. Виявлено їх переваги та недоліки, що дозволило визначити пріоритетність подальших досліджень та можливі перспективні шляхи вирішення поставлених завдань.

Ключові слова: безпілотні літальні апарати; безпека; система ADS-B; кібератаки; захист даних.